

# On coordinatising planes of prime power order using finite fields

Robert S. Coulter

520 Ewing Hall  
Department of Mathematical Sciences  
University of Delaware  
Newark, DE, USA, 19716

September 7, 2016

## Abstract

We revisit the coordinatisation method for projective planes. First, we discuss how the behaviour of the additive and multiplicative loops can be described in terms of its action on the “vertical” line, and how this means one can coordinatise certain planes in an optimal sense. We then move to consider projective planes of prime power order only. Specifically, we consider how coordinatising planes of prime power order using finite fields as the underlying labelling set leads to some general restrictions on the form of the resulting planar ternary ring (PTR) when viewed as a trivariate polynomial over the field. We also consider the Lenz-Barlotti type of the plane being coordinatised, deriving further restrictions on the form of the PTR polynomial.

## 1 Introduction

This paper is concerned with two interlinked areas in the study of projective planes – namely the coordinatisation method and the Lenz-Barlotti classification. The coordinatisation method takes an arbitrary projective plane and produces a trivariate function known as a *planar ternary ring (PTR)* over whatever set is used as the labelling set during the coordinatisation process. The Lenz-Barlotti (LB) classification is a coarse classification system for affine and projective planes centred on the transitive behaviour exhibited by the full automorphism group of the plane.

We begin by outlining the coordinatisation method using slightly non-standard diagrams, and describe how this leads to the concept of a planar ternary ring (PTR). From the PTR so constructed it is common to define an “additive” and a “multiplicative” loop. Through the use of our diagrams, we can give an explicit

description of the action of these loops on the vertical line. We have dual motivations in this initial discussion. In the long term, our motivation is a desire to give a meaningful definition of “optimal coordinatisation”, and this is achieved through our understanding of these actions. In the short term, our motivation is to give an additional insight into a well known conjecture in projective geometry concerning Fano configurations. It has been known for some time that a finite Desarguesian plane contains a Fano configuration if and only if the plane has even order. For non-Desarguesian planes, a folk-lore conjecture claims that all finite non-Desarguesian planes must contain a Fano configuration. (Though the conjecture has been attributed to Hanna Neumann, she did not make the conjecture.) In support of the conjecture, several classes of planes have been shown to contain Fano configurations; for a non-exhaustive set of examples see Neumann [13], Rahilly [15], Johnson [9], or Petrak [14]. Here we note that the action of the additive loop on the vertical line provides an obvious necessary and sufficient condition for the existence of a Fano configuration in a projective plane, though the utility of these conditions to prove the conjecture is unclear.

We then concentrate on the coordinatisation of projective planes of prime power order. (Of course, anyone who believes the prime-power conjecture is true would view this as no restriction at all; the present author is not willing to express any view on that conjecture’s validity, at least not in print!) Specifically, we here instigate a study of projective planes of prime power order via their coordinatisation over finite fields of the appropriate order. In this way we are able to view the resulting PTR as a reduced trivariate polynomial over a finite field, what we call a *PTR polynomial*. We then derive restrictions on the form of the PTR polynomial using the functional properties that any PTR must exhibit. As shall be seen, several forms of reduced permutation polynomials and  $\kappa$ -polynomials (both of which we shall define below) naturally arise from this relation. The culmination of the results of this section, and the main statement in this general situation, is given in Theorem 13.

Finally, we outline the Lenz-Barlotti classification system for projective planes. It is generally well known that knowledge of the Lenz-Barlotti type of a projective plane  $\mathcal{P}$  can lead to additional algebraic properties of the PTR obtained from coordinatising it, but this only occurs when some effort is made to coordinatise the plane in an optimal way. We make explicit what we mean by optimal coordinatisation, and utilise this concept to obtain further restrictions on the form of the PTR polynomial under various assumptions concerning the LB type. In particular, we show how one can coordinatise suitable planes so that either the additive or multiplicative loop resulting from the coordinatisation is exactly the same as its corresponding field operation, and consider how this can affect the form of the PTR polynomial. Theorems 16 and 18 are the main results of this section.

The paper is set out as follows. In Section 2, we give an overview of the coordinatisation approach, and discuss the actions of the loops on the vertical line. There we also discuss the conjecture on the existence of Fano configurations. In Section 3 we restrict the coordinatisation process to planes of prime power order and where the coordinatising set used is a finite field, and describe

explicitly how a PTR polynomial is produced. Section 4 then provides a sequence of results on the behaviour and form of PTR polynomials. In the final section, we turn to a discussion of the Lenz-Barlotti classification for projective planes and affine planes. There we make explicit the concept of an “optimal” coordinatisation of a plane, and exploit this idea to produce further restrictions on the PTR polynomial based on knowledge of the LB type of the projective plane when coordinatised optimally.

## 2 Coordinatisation

The method of coordinatisation has been used now for over seventy years. There are at least 3 standard coordinatisation methods. Though they are all essentially equivalent, they produce slightly different properties in the resulting PTRs. For the sake of consistency, we shall use the process outlined by Hughes and Piper in [8], Chapter 5 – they give the two other methods at the end of that same chapter. In this section we will describe precisely the coordinatisation method for introducing a coordinate system for an abstract projective plane. While there are several readily available sources for describing this method, our motivation for providing another treatment is twofold: firstly, there is the desire for a self-contained discussion, and secondly, we will use diagrams which are not standard elsewhere with the explicit aim of making it easier to visualise certain concepts we wish to discuss.

Let  $\mathcal{P}$  be a projective plane of order  $n$  and let  $\mathcal{R}$  be any set of cardinality  $n$  – this set along with the symbol  $\infty$  will be all that is required to produce a coordinate system for the plane. We designate two special elements of  $\mathcal{R}$  by 0 and 1 for reasons which will become clear. We now proceed to coordinatise  $\mathcal{P}$ .

- Choose any triangle in the plane  $\mathbf{O}, \mathbf{x}, \mathbf{y}$ . Label  $\mathbf{O} = (0, 0)$ ,  $\mathbf{x} = (0)$  and  $\mathbf{y} = (\infty)$  – by doing so we have now determined the “line at infinity”  $\overline{\mathbf{x}\mathbf{y}} = [\infty]$ . We also set  $[0] = \overline{\mathbf{O}\mathbf{y}}$  and  $[0, 0] = \overline{\mathbf{O}\mathbf{x}}$ . (The process for an affine plane  $\mathcal{A}$  differs from the projective version only in that the line at infinity is pre-determined, so that the choice of points  $\mathbf{x}$  and  $\mathbf{y}$  is restricted.)
- A fourth point,  $\mathbf{I}$ , not collinear with any two of  $\mathbf{O}, \mathbf{x}, \mathbf{y}$  is now chosen and labelled  $\mathbf{I} = (1, 1)$ .
- To finalise the initialisation process, we label some obvious intersection points:
  - Set  $\overline{\mathbf{x}\mathbf{I}} \cap [0] = (0, 1)$ .
  - Set  $\overline{\mathbf{y}\mathbf{I}} \cap [0, 0] = (1, 0)$ .
  - Set  $\overline{(1, 0)(0, 1)} \cap [\infty] = \mathbf{J} = (1)$ .

The situation after this initial phase is given in Figure 1.

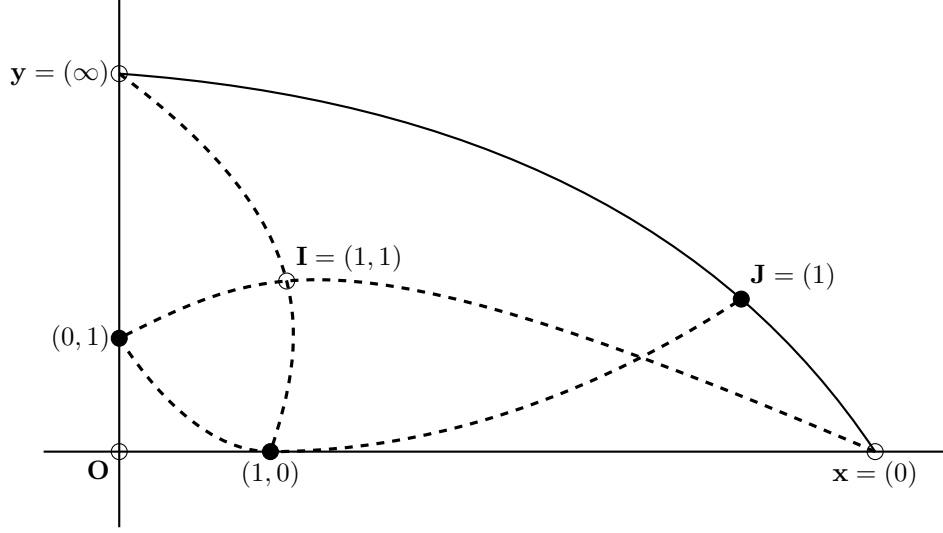


Figure 1: After the initial labelling.

At this point, we have labelled 3 of the  $n + 1$  points of both of the lines  $[0]$  and  $[0, 0]$ . One may now label the remaining  $n - 2$  points of  $[0]$  as  $(0, a)$  in arbitrary way using the remaining  $n - 2$  elements  $a \in \mathcal{R} \setminus \{0, 1\}$ . This is the last remaining freedom of choice in the process, as from this stage onwards, the coordinates of all points and lines are totally determined. Later in this section we will explain how the additive and multiplicative loops that result from the coordinatising procedure can be seen to act on  $\overline{Oy}$ , thus outlining how the elements of  $\mathcal{R}$  interact under these operations follows from this random labelling.

We now proceed to label all points and lines of the plane; see Figure 2.

- To label the remaining points of  $[0, 0]$  we set  $\overline{(0, a)J} \cap [0, 0] = (a, 0)$ .
- To label the remaining points of  $[\infty]$  we set  $\overline{(0, a)(1, 0)} \cap [\infty] = (a)$ .
- To label the remaining “affine” points we set  $\overline{(a, 0)y} \cap \overline{(0, b)x} = (a, b)$ .

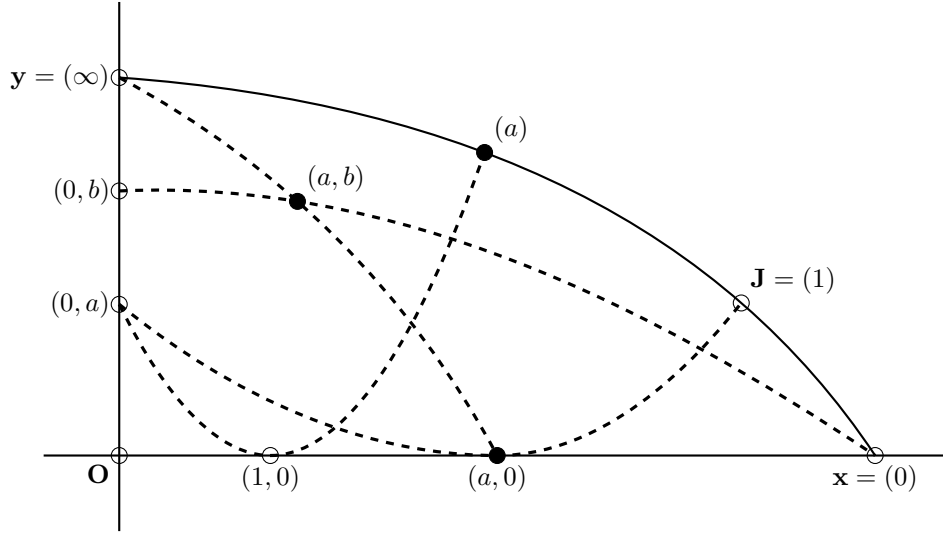


Figure 2: Point labelling.

With a labelling of the points complete, it remains only to give a labelling of the lines (Figure 3).

- To label the “vertical” lines we set  $\overline{(a, 0) \mathbf{y}} = [a]$ .
- To label the “lines of slope  $m$ ” we set  $\overline{(m)(0, k)} = [m, k]$ .

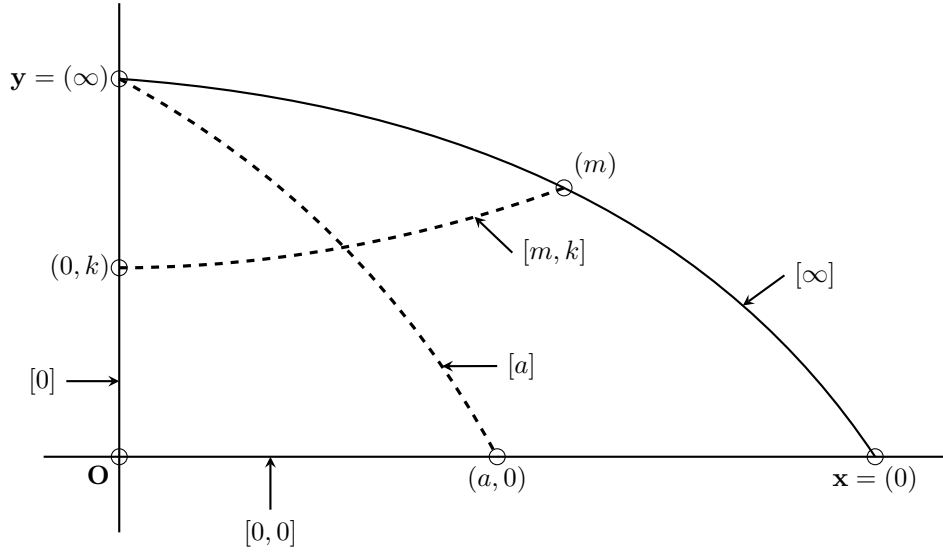


Figure 3: Line labelling.

From this coordinatisation, one now defines a tri-variate function  $T$  on  $\mathcal{R}$ , called a *planar ternary ring (PTR)*, by setting  $T(m, x, y) = k$  if and only if  $(x, y) \in$

$[m, k]$ . This PTR will exhibit certain properties and is actually equivalent to the projective plane as any three variable function exhibiting those properties can be used to define a projective plane. More precisely, we have the following important result, essentially due to Hall [6]; see also Hughes and Piper, [8], Theorem 5.1.

**Lemma 1** (Hall, [6], Theorem 5.4). *Let  $\mathcal{P}$  be a projective plane of  $n$  and  $\mathcal{R}$  be any set of cardinality  $n$ . Let  $T : \mathcal{R}^3 \rightarrow \mathcal{R}$  be a PTR obtained from coordinatising  $\mathcal{P}$ . Then  $T$  must satisfy the following properties:*

- (a)  $T(a, 0, z) = T(0, b, z) = z$  for all  $a, b, z \in \mathcal{R}$ .
- (b)  $T(x, 1, 0) = x$  and  $T(1, y, 0) = y$  for all  $x, y \in \mathcal{R}$ .
- (c) If  $a, b, c, d \in \mathcal{R}$  with  $a \neq c$ , then there exists a unique  $x$  satisfying  $T(x, a, b) = T(x, c, d)$ .
- (d) If  $a, b, c \in \mathcal{R}$ , then there is a unique  $z$  satisfying  $T(a, b, z) = c$ .
- (e) If  $a, b, c, d \in \mathcal{R}$  with  $a \neq c$ , then there is a unique pair  $(y, z)$  satisfying  $T(a, y, z) = b$  and  $T(c, y, z) = d$ .

Conversely, any tri-variate function  $T$  defined on  $\mathcal{R}$  which satisfies Properties (c) through (e) can be used to define an affine plane  $\mathcal{A}_T$  of order  $q$  as follows:

- the points of  $\mathcal{A}$  are  $(x, y)$ , with  $x, y \in \mathcal{R}$ ;
- the lines of  $\mathcal{A}$  are the symbols  $[m, a]$ , with  $m, a \in \mathcal{R}$ , defined by

$$[m, a] = \{(x, y) \in \mathcal{R} \times \mathcal{R} : a = T(m, x, y)\},$$

and the symbols  $[c]$ , with  $c \in \mathcal{R}$ , defined by

$$[c] = \{(c, y) : y \in \mathcal{R}\}.$$

Since one only needs Properties (c) through (e) to construct  $\mathcal{P}$ , a polynomial satisfying just the latter three properties is called a *weak PTR*. If a weak PTR also satisfies (a) (resp. (b)), then it is a *weak PTR with zero* (resp. *weak PTR with unity*).

It is customary to define an addition  $\oplus$  and multiplication  $\odot$  by

$$\begin{aligned} x \oplus y &= T(1, x, y), \\ x \odot y &= T(x, y, 0), \end{aligned}$$

for all  $x, y \in \mathcal{R}$ . It is well known that the properties of the plane guarantee that both  $\oplus$  and  $\odot$  are loops with identities 0 and 1 over  $\mathcal{R}$  and  $\mathcal{R}^*$ , respectively. A PTR is called *linear* over  $\mathcal{R}$  if  $T(x, y, z) = (x \odot y) \oplus z$  for all  $x, y, z \in \mathcal{R}$  – that is, if  $T$  can be reconstructed from only knowing the operations  $\oplus$  and  $\odot$ . One point of interest here is how the operations  $\oplus$  and  $\odot$  act on the vertical line  $[0] = \overline{\mathbf{0y}}$ ; we shall outline this action directly. Before doing so, we mention an

important example. Consider the polynomial  $T(X, Y, Z) = XY + Z$ . It is easily checked that the polynomial  $T$  is a linear PTR over any field  $\mathcal{K}$ ; it defines the Desarguesian plane in every case. It cannot be over emphasised that the same plane can yield many different PTRs as choosing different quadrangles as the reference points  $\mathbf{O}, \mathbf{x}, \mathbf{y}$  and  $\mathbf{I}$ , may yield very different PTRs. We discuss this further in Section 5.

## 2.1 The action of $(\mathcal{R}, \oplus)$ on $\overline{\mathbf{O}\mathbf{y}}$

Let us first consider  $(\mathcal{R}, \oplus)$ . The process is anchored by our initial triangle  $\mathbf{O}, \mathbf{x}, \mathbf{y}$  and the point  $\mathbf{J} = (1)$ .

- Choose two points  $(0, a), (0, b)$  on  $\overline{\mathbf{O}\mathbf{y}} = [0]$ .
- Create the point  $(a, 0) = \overline{(0, a)\mathbf{J}} \cap \overline{\mathbf{O}\mathbf{x}}$ .
- Next create the point  $(a, b) = \overline{(a, 0)\mathbf{y}} \cap \overline{(0, b)\mathbf{x}}$ .
- Now consider the point  $(0, k) = \overline{\mathbf{J}(a, b)} \cap \overline{\mathbf{O}\mathbf{y}}$ . It lies on the line  $[1, k]$  by construction. Furthermore, from the definition of the PTR and  $\oplus$  we see  $k = T(1, a, b) = a \oplus b$ . Thus  $(0, k) = (0, a \oplus b)$ .

Pictorially, the action of  $\oplus$  on the vertical line is seen in Figure 4.

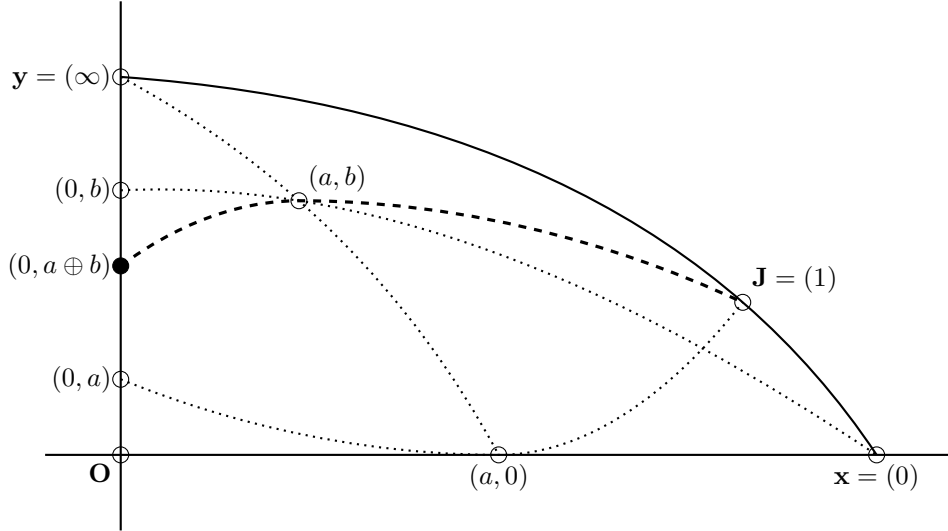


Figure 4: Action of the additive loop on the vertical line.

## 2.2 The action of $(\mathcal{R}^*, \odot)$ on $\overline{\mathbf{O}\mathbf{y}}$

As with the operation  $\oplus$ , the process by which the action of  $(\mathcal{R}^*, \odot)$  on  $\overline{\mathbf{O}\mathbf{y}}$  is described relies on our initial triangle  $\mathbf{O}, \mathbf{x}, \mathbf{y}$  and the point  $\mathbf{J} = (1)$ . We'll also need the point  $(1, 0)$ .

- Choose two points  $(0, a), (0, b)$  on  $\overline{\mathbf{O}\mathbf{y}} = [0]$ .
- Create the point  $(b, 0) = \overline{(0, b)\mathbf{J}} \cap \overline{\mathbf{O}\mathbf{x}}$ .
- Create the point  $(a) = \overline{(0, a)(1, 0)} \cap \overline{\mathbf{x}\mathbf{y}}$ .
- Now consider the point  $(0, k) = \overline{(a)(b, 0)} \cap \overline{\mathbf{O}\mathbf{y}}$ . It lies on the line  $[a, k]$  by construction. Furthermore, from the definition of the PTR and  $\odot$  we see  $k = T(a, b, 0) = a \odot b$ . Thus  $(0, ) = (0, a \odot b)$ .

This action is represented in Figure 5.

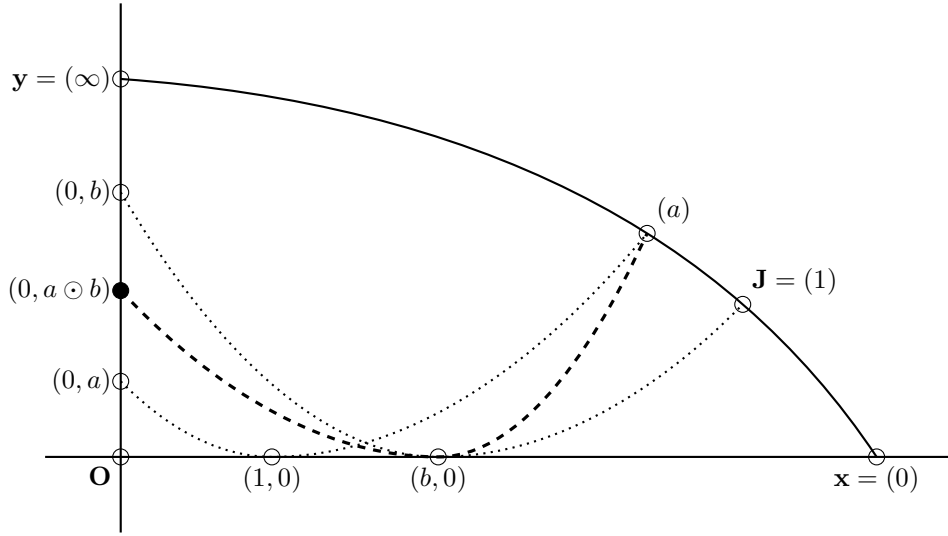


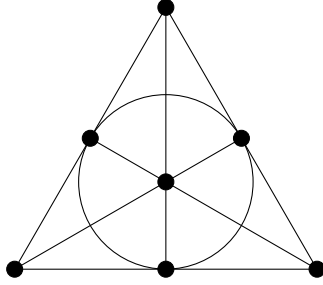
Figure 5: Action of the multiplicative loop on the vertical line.

### 2.3 Fano configurations in projective planes

As an aside before moving to the main motivation for this article, we first provide a theorem concerning a well known conjecture in projective geometry. It is possible, perhaps even probable given the simplicity of our argument, that the main theorem of this section is known, but we have not been able to locate it.

The Fano configuration must be one of the most oft drawn graphs in all of mathematics. Here it is (again!):





Using the action of the additive loop on the vertical line described above, here we establish a necessary and sufficient condition for any projective plane to contain a Fano configuration.

**Theorem 2.** *Let  $\mathcal{P}$  be a projective plane of finite order. Then  $\mathcal{P}$  contains a Fano configuration if and only if it can be coordinatised in such a way that the resulting additive loop contains an involution.*

*Proof.* Suppose first that the plane  $\mathcal{P}$  has been coordinatised in such a way that the resulting additive loop,  $(\mathcal{R}, \oplus)$ , contains an involution. Call it  $t$ . Then  $t \oplus t = 0$ , so that  $(0, t \oplus t) = (0, 0) = \mathbf{O}$ . In particular,  $\mathbf{O}, (t, t)$  and  $\mathbf{J}$  are collinear. If we now return to the diagram describing how addition acts on  $\overline{\mathbf{O}\mathbf{y}}$  and redraw, we find we have the following scenario:

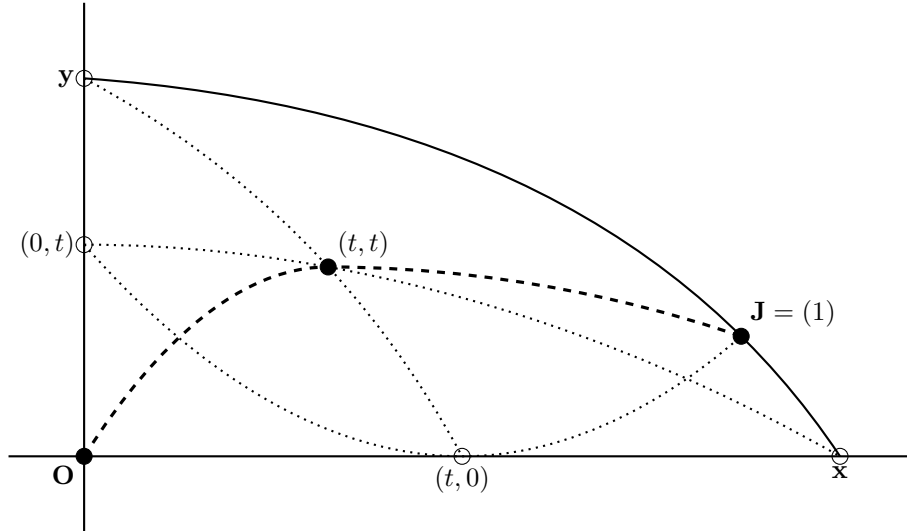


Figure 6: Collinearity of  $\mathbf{O}$ ,  $(t, t)$  and  $\mathbf{J}$ .

This is easily seen to be a Fano configuration.

Conversely, suppose a projective plane  $\mathcal{P}$  contains a Fano configuration. Let  $\mathcal{R}$  be our coordinatising set and  $t \in \mathcal{R}^*$  be fixed. Choose any triangle  $\mathbf{O}, \mathbf{x}, \mathbf{y}$  of the Fano configuration. Of the remaining four points in the Fano configuration, three must lie on a line: label them  $(0, t)$ ,  $(t, 0)$  and  $\mathbf{J} = (1)$ , with  $(0, t)$  on

$\overline{\mathbf{Oy}}$ ,  $(t, 0)$  on  $\overline{\mathbf{Ox}}$  and  $\mathbf{J}$  on  $\overline{\mathbf{x}\mathbf{y}}$ . Finally, label the remaining point  $(t, t)$ . If we chose  $t = 1$ , then we have already selected  $\mathbf{I} = (1, 1)$  and coordinatising  $\mathcal{P}$  using the quadrangle  $\mathbf{OxyI}$  will result with  $1 \oplus 1 = 0$ . Otherwise, choose an arbitrary point  $\mathbf{I} = (1, 1)$  not in the Fano configuration and set  $\overline{\mathbf{IJ}} \cap \overline{\mathbf{Ox}} = (1, 0)$  and  $\overline{\mathbf{IJ}} \cap \overline{\mathbf{Oy}} = (0, 1)$ . Now proceeding to coordinatise  $\mathcal{P}$  using the quadrangle  $\mathbf{OxyI}$ , we find  $t \oplus t = 0$ . In either case we have an involution in  $(\mathcal{R}, \oplus)$ .  $\square$

An immediate corollary of the theorem is the statement concerning Fano configurations in Desarguesian planes mentioned in the introduction: in a Desarguesian plane, any coordinatisation must produce an additive loop that is, in fact, a group of order equal to the order of the plane. Consequently, the plane must have even order to allow an involution and no Desarguesian plane of odd order can contain a Fano configuration.

While the statement gives a clear necessary and sufficient condition, it may still be viewed as unsatisfying, in that there is no known general criteria which determine that a loop must contain an involution.

We note that one direction of the above theorem is immediate from the following general statement.

**Theorem 3.** *Let  $\mathcal{P}$  be a projective plane of order  $n$  and  $\mathcal{S}$  be a subplane of  $\mathcal{P}$  of order  $m \leq n$ . Let  $\mathcal{R}$  be a coordinatising set for  $\mathcal{P}$  of cardinality  $n$ . If the coordinatising quadrangle  $\mathbf{OxyI}$  is contained in  $\mathcal{S}$ , then there exists a subset  $\mathcal{S}$  of  $\mathcal{R}$  of cardinality  $m$  which acts as the coordinatising set of  $\mathcal{S}$ . Moreover, the PTR  $T$  produced by coordinatising  $\mathcal{P}$  acts as the PTR of  $\mathcal{S}$  when restricted to  $\mathcal{S}$ .*

The proof follows immediately from the observation that after choosing the quadrangle  $\mathbf{OxyI}$  from  $\mathcal{S}$ , the sequential way in which coordinates are assigned guarantees you could simply coordinatise  $\mathcal{S}$  first during the coordinatisation of  $\mathcal{P}$  (or, indeed, you could just as easily label the points of  $\mathcal{S}$  last). Since the coordinatisation of a Desarguesian plane must always produce a field under the loop operations arising from the coordinatisation, we get the following corollary for free.

**Corollary 4.** *If  $\mathcal{P}$  is a projective plane of order  $n$  containing a Desarguesian subplane of order  $q$ , then  $\mathcal{P}$  can always be coordinatised so that there is a subset  $\mathcal{S}$  of the coordinatising set which forms a field of order  $q$  under the operations  $\oplus$  and  $\odot$  arising from the coordinatisation of  $\mathcal{P}$ .*

### 3 Coordinatising using finite fields

Throughout the remainder of the paper we fix  $q = p^e$  for some prime  $p$  and natural number  $e$ . We use  $\mathbb{F}_q$  to denote the finite field of  $q$  elements and  $\mathbb{F}_q^*$  its non-zero elements. Every function on  $\mathbb{F}_q$  can be represented uniquely by a polynomial in  $\mathbb{F}_q[X]$  of degree less than  $q$ ; this follows at once from Lagrange Interpolation, and indeed this observation is easily extended to the multivariate case. Any polynomial whose degree in each variable is less than  $q$  is called *reduced*. A polynomial  $f \in \mathbb{F}_q[X_1, \dots, X_n]$  is called a *permutation polynomial*

(PP) over  $\mathbb{F}_q$  if the evaluation map  $\mathbf{x} \mapsto f(\mathbf{x})$  is equidistributive on  $\mathbb{F}_q$  – that is, for each  $y \in \mathbb{F}_q$ , the equation  $f(\mathbf{x}) = y$  has  $q^{n-1}$  solutions  $\mathbf{x} \in \mathbb{F}_q^n$ . (In the case where  $n = 1$ , the evaluation map is a bijection.) It follows from Hermite’s criteria that if a reduced polynomial  $f \in \mathbb{F}_q[X_1, \dots, X_n]$  is a PP over  $\mathbb{F}_q$ , then the degree of  $f$  in each  $X_i$  is at most  $q - 2$ . Even a casual perusal of Mathematical Reviews will show PPs have been a significant research topic in their own right for many years (effectively since historical times), with a wide array of applications.

A related concept also of interest is that of a  $\kappa$ -polynomial. A polynomial  $f \in \mathbb{F}_q[X_1, \dots, X_n]$  is a  $\kappa$ -polynomial over  $\mathbb{F}_q$  if

$$k_a = \#\{\mathbf{x} \in \mathbb{F}_q^n : \mathbf{f}(\mathbf{x}) = \mathbf{a}\}$$

is independent of  $a$  for  $a \in \mathbb{F}_q^*$ . In direct contrast to the study of permutation polynomials, there are almost no results in the literature directly discussing  $\kappa$ -polynomials. This seems altogether surprising since the specified regularity on preimages of all non-zero elements of the field suggests such polynomials must almost certainly appear in many guises. As an example in how they may arise, recall that a *skew Hadamard difference set* (SHDS)  $D \subset \mathbb{F}_q^*$  is a set of order  $(q - 1)/2$  where every element of  $\mathbb{F}_q^*$  can be written as a difference of elements of  $D$  in precisely  $(q - 3)/4$  ways. Let  $D$  be any SHDS, and define a two-to-one map  $\phi : \mathbb{F}_q^* \rightarrow D$  in an arbitrary way. Extending  $\phi$  to all of  $\mathbb{F}_q$  by setting  $\phi(0) = 0$ , we can associate with  $\phi$  a reduced polynomial  $f \in \mathbb{F}_q[X]$ . It is straightforward to confirm the polynomial  $M(X, Y) = f(X) - f(Y)$  is a  $\kappa$ -polynomial over  $\mathbb{F}_q$  with  $k_a = q - 1$  for all  $a \in \mathbb{F}_q^*$ . (One could generalise this construction in a suitable way to obtain  $\kappa$ -polynomials in more than two variables using difference families.) The thesis of Matthews, [11], contains some general results on  $\kappa$ -polynomials. Some of these results are given in the author’s Section 9.4 of the Handbook of Finite Fields [12]. Theorem 9.4.8 of [12], which is straightforward to prove, shows how  $\kappa$ -polynomials play a role in the study of projective planes; the theorem is extended in Theorem 9 below.

One can choose any set  $\mathcal{R}$  of cardinality  $n$  for the labelling of points in the coordinatisation process, but since the coordinatisation method will produce an algebraic structure on the set chosen, there are obviously good and bad choices. The resulting function will often exhibit additional algebraic structure, inherited from the plane, so algebraic sets are obvious candidates. For example, regardless of the plane, the points  $\mathbf{0}$  and  $\mathbf{1}$  determine two special elements, zero and one, respectively, of the coordinatisation which have properties much the same to 0 and 1 in any ring with unity. Since the labelling during the coordinatisation process is arbitrary, by choosing a ring of order  $n$  with unity, we may label the zero and one of the coordinatisation as the 0 and 1 of the ring.

We now move to make the previous paragraph much more formal in the case where the plane has prime power order  $q$ . Let  $\mathcal{P}$  be a projective plane of order  $q$ . Via coordinatisation, we can obtain a PTR equivalent to the plane  $\mathcal{P}$ . Since the plane has order  $q$ , we can view the PTR as some function in three variables defined over  $\mathbb{F}_q$ , and consequently view the function as a (reduced)

polynomial  $T \in \mathbb{F}_q[X, Y, Z]$ . Furthermore, since the correspondence of elements in the coordinatisation and the elements of  $\mathbb{F}_q$  is arbitrary, we may set the zero and one of the coordinatisation of  $\mathcal{P}$  to be the elements 0 and 1 of  $\mathbb{F}_q$ .

**Definition 5.** A PTR polynomial  $T(X, Y, Z)$  over  $\mathbb{F}_q$  is any three variable polynomial in  $\mathbb{F}_q[X, Y, Z]$  resulting from the coordinatisation of a plane  $\mathcal{P}$  of order  $q$  through labelling the points of  $\mathcal{P}$  using elements of  $\mathbb{F}_q$  and where we label  $\mathbf{O} = (0, 0)$  and  $\mathbf{I} = (1, 1)$ .

Note that for a PTR polynomial, we are guaranteed that the zero and one of the PTR and the 0 and 1 of  $\mathbb{F}_q$  coincide. An equivalent definition is that  $T \in \mathbb{F}_q[X, Y, Z]$  is a PTR polynomial over  $\mathbb{F}_q$  if it satisfies Properties (a) through (e) of Lemma 1 over  $\mathbb{F}_q$ .

## 4 Restrictions on the form of PTR polynomials

We now look to exploit the conditions on  $T$  described in Lemma 1 to obtain restrictions on the possible forms of  $T$ . Throughout we assume  $T$  is a reduced polynomial.

**Theorem 6.** Suppose  $T \in \mathbb{F}_q[X, Y, Z]$  satisfies Property (a). Then

$$T(X, Y, Z) = Z + XYZ M_1(X, Y, Z) + M_2(X, Y), \quad (1)$$

where

$$M_1(X, Y, Z) = \sum_{i=0}^{q-2} \sum_{j=0}^{q-2} \sum_{k=0}^{q-2} b_{ijk} X^i Y^j Z^k,$$

$$M_2(X, Y) = \sum_{i=1}^{q-1} \sum_{j=1}^{q-1} c_{ij} X^i Y^j.$$

In particular,

$$x \odot y = T(x, y, 0) = M_2(x, y) \quad (2)$$

for all  $x, y \in \mathbb{F}_q$ .

*Proof.* As a polynomial, we may represent  $T$  as

$$T(X, Y, Z) = \sum_{i,j,k=0}^{q-1} a_{ijk} X^i Y^j Z^k.$$

By Property (a),  $T(0, 0, z) = z$  for all  $z$ . Viewing this as a polynomial identity in  $Z$  we immediately find

$$a_{00k} = \begin{cases} 1 & \text{if } k = 1, \\ 0 & \text{if } k \neq 1. \end{cases}$$

Noting  $T(x, 0, Z) = Z$  for all  $x$ , we again view this as a polynomial identity in  $X, Z$ , and obtain

$$Z = T(X, 0, Z) = \sum_{i=0}^{q-1} X^i \left( \sum_{k=0}^{q-1} a_{i0k} Z^k \right).$$

For  $i \neq 0$ , this now forces

$$\sum_{k=0}^{q-1} a_{i0k} Z^k = 0.$$

As a polynomial identity, we get  $a_{i0k} = 0$  for all  $i \neq 0$ . A similar argument shows  $a_{0jk} = 0$  for all  $j \neq 0$ . Hence

$$T(X, Y, Z) = Z + \sum_{i,j=1}^{q-1} \sum_{k=0}^{q-1} a_{ijk} X^i Y^j Z^k = Z + XY T_1(X, Y, Z), \quad (3)$$

for some reduced  $T_1 \in \mathbb{F}_q[X, Y, Z]$ . It is clear we can now rewrite  $T_1$  as claimed in (1).  $\square$

So we see that Property (a) alone isolates the behaviour of  $\odot$ , though of course it does not *define* the behaviour of  $\odot$ .

We now derive a result on PPs; though this could just as easily be established by considering the plane directly, we choose instead to use as few of the properties of Lemma 1 as is necessary in each case.

**Theorem 7.** *Let  $T \in \mathbb{F}_q[X, Y, Z]$ . The following statements hold.*

- (i) *Suppose  $T$  satisfies Properties (a) and (c). Then  $T(X, y, z)$  is a PP in  $X$  for every choice of  $(y, z) \in \mathbb{F}_q^* \times \mathbb{F}_q$ .*
- (ii) *Suppose  $T$  satisfies Properties (a) and (e). Then  $T(x, Y, z)$  is a PP in  $Y$  for every choice of  $(x, z) \in \mathbb{F}_q^* \times \mathbb{F}_q$ .*
- (iii) *Suppose  $T$  satisfies Property (d). Then  $T(x, y, Z)$  is a PP in  $Z$  for every choice of  $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$ .*

*Proof.* For the 1st claim, an appeal to Property (c) with  $c = 0 \neq a, b, d$  arbitrary shows the equation  $T(x, a, b) = T(x, 0, d)$  has a unique solution  $x$ . By Property (a),  $T(x, 0, d) = d$ , and so  $T(x, a, b) = d$  has a unique solution  $x$  for each  $d \in \mathbb{F}_q$ .

For (ii), fix  $a = 0$ . By Property (e), for any  $b, c, d$  with  $c \neq 0$  there exists a unique  $(y, z)$  such that  $T(0, y, z) = b$  and  $T(c, y, z) = d$ . By Property (a),  $T(0, y, z) = z$ , and so  $z$  is fixed:  $z = b$ . Thus, as we range over all  $d \in \mathbb{F}_p$ , we have a unique preimage  $y$ , proving the claim.

For (iii), fix  $x, y$ . Property (d) tells us that for any  $c$ , we can always solve uniquely for  $z$  in  $T(x, y, z) = c$ . Thus  $T(x, y, z_1) = T(x, y, z_2)$  implies  $z_1 = z_2$ , so that  $T(x, y, Z)$  is a PP in  $Z$  for every  $x, y$ .  $\square$

**Corollary 8.** *Suppose  $T \in \mathbb{F}_q[X, Y, Z]$  satisfies Properties (a), (c), (d) and (e). Then  $T$  has degree at most  $q - 2$  in each of  $X$ ,  $Y$ , and  $Z$ .*

*Proof.* By assumption,  $T$  has the form given in (1). Since  $T(x, y, Z)$  is a PP for all  $x, y \in \mathbb{F}_q$ , Hermite's criteria tells us

$$\sum_{i,j=1}^{q-1} a_{ij(q-1)} x^i y^j = 0$$

for all  $x, y$ . This holds as a polynomial identity in  $X, Y$ , and so  $b_{ij(q-1)} = 0$  for all  $i, j$ . Similar arguments can be obtain the bounds on the degrees of  $X$  and  $Y$ .  $\square$

While it may be tempting to surmise from the above that  $T(X, Y, z)$  is a PP for all  $z \in \mathbb{F}_q$ , it is not actually true, as the next result shows.

**Theorem 9.** *Suppose  $T \in \mathbb{F}_q[X, Y, Z]$  satisfies Property (a) and one of Properties (c) or (e). Then  $T(X, Y, z) - z$  is a  $\kappa$ -polynomial for any  $z \in \mathbb{F}_q$ .*

*Proof.* Fix  $z$  and consider the polynomial  $f_z \in \mathbb{F}_q[X, Y]$  given by  $f_z(X, Y) = T(X, Y, z)$ . If  $d = z$ , then by Property (a),  $T(0, y, z) = T(x, 0, z) = d$  for all  $x, y \in \mathbb{F}_q$ . Thus  $f_z(x, y) = d$  has (at least)  $2q - 1$  solutions. If  $d \neq z$ , then by Theorem 7 (i) or (ii), there are precisely  $q - 1$  solutions  $(x, y) \in \mathbb{F}_q^* \times \mathbb{F}_q^*$  to the equation  $f_z(x, y) = d$ . Since this accounts for all  $q^2$  images, we see

$$f_z(x, y) = d \quad \begin{cases} \text{has } q - 1 \text{ solutions when } d \neq z, \\ \text{has } 2q - 1 \text{ solutions when } d = z. \end{cases}$$

Consequently, the polynomial  $f_z(X, Y) - z = T(X, Y, z) - z$  is a  $\kappa$ -polynomial over  $\mathbb{F}_q$ .  $\square$

**Corollary 10.** *Suppose  $T \in \mathbb{F}_q[X, Y, Z]$  satisfies either Property (a) and one of Properties (c) or (e); or Property (d). Then  $T(X, Y, Z)$  is a PP over  $\mathbb{F}_q$ .*

*Proof.* Suppose first that  $T$  satisfies Property (a) and one of Properties (c) or (e). Fixing  $z, d \in \mathbb{F}_q$ , we see from the proof of Theorem 9 that

$$T(x, y, z) = d \quad \begin{cases} \text{has } q - 1 \text{ solutions when } z \neq d, \\ \text{has } 2q - 1 \text{ solutions when } z = d. \end{cases}$$

Consequently, as we range over all  $z \in \mathbb{F}_q$ , a given  $d$  has  $(2q - 1) + (q - 1)(q - 1) = q^2$  preimages  $(x, y, z) \in \mathbb{F}_q^3$ .

Now suppose Property (d) is satisfied. Then by Theorem 7 (iii),  $T(x, y, Z)$  is a PP for all choices of  $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$ . It follows at once that  $T(x, y, z) = d$  has precisely  $q^2$  solutions  $(x, y, z)$ .  $\square$

At this point, we have shown that Properties (a), (c), and (d) can lead to PPs. Property (e) can also be used to derive a PP result, but not over  $\mathbb{F}_q$ . Suppose  $T \in \mathbb{F}_q[X, Y, Z]$ . Let  $\{1, \beta\}$  be a basis for  $\mathbb{F}_{q^2}$  over  $\mathbb{F}_q$ . For any  $a, b \in \mathbb{F}_q$ , we define the function  $S_{a,b} : \mathbb{F}_{q^2} \rightarrow \mathbb{F}_{q^2}$  by

$$S_{a,b}(x) = S_{a,b}(y + \beta z) = T(a, y, z) + \beta T(b, y, z).$$

When we talk of the polynomial  $S_{a,b}$  we will mean the polynomial of least degree in  $\mathbb{F}_{q^2}[X]$  which when induced produces the function just defined. The following lemma is now immediate.

**Lemma 11.** *Suppose  $T \in \mathbb{F}_q[X, Y, Z]$  satisfies Property (e). Then  $S_{a,b}$  is a permutation polynomial over  $\mathbb{F}_{q^2}$  whenever  $a \neq b$ .*

Finally we move to consider how Property (b) impacts the form of the PTR polynomial. We have already seen how Property (a) alone isolates the behaviour of  $\odot$ , see (2) above. One interesting outcome of combining Properties (a) and (b) is that the behaviour of  $\oplus$  is also isolated.

**Lemma 12.** *Suppose  $T \in \mathbb{F}_q[X, Y, Z]$  satisfies Properties (a) and (b). Then  $T$  has the shape (1) and*

$$\sum_{i=1}^{q-1} c_{ij} = \sum_{i=1}^{q-1} c_{ji} = \begin{cases} 1 & \text{if } j = 1, \\ 0 & \text{if } j > 1. \end{cases}$$

Moreover,

$$y \oplus z = T(1, y, z) = y + z + yz M_1(1, y, z) \quad (4)$$

for all  $y, z \in \mathbb{F}_q$ .

*Proof.* From Property (b), we know  $T(X, 1, 0) = X$ . Combining this polynomial identity with (1) forces the first set of conditions on the coefficients, while using  $T(1, Y, 0) = Y$  forces the second set. In addition, applying  $T(1, y, 0) = y$  to (1), we also find  $T(1, y, z) = y + z + yz M_1(1, y, z)$ , as claimed.  $\square$

Now, if we combine all of the above, we obtain the following result about PTR polynomials, the proof of which is immediate from the above statements.

**Theorem 13.** *Suppose  $T(X, Y, Z)$  is a PTR polynomial over  $\mathbb{F}_q$ . Then*

$$T(X, Y, Z) = Z + XYZ M_1(X, Y, Z) + M_2(X, Y), \quad (5)$$

with

$$M_1(X, Y, Z) = \sum_{i=0}^{q-3} \sum_{j=0}^{q-3} \sum_{k=0}^{q-3} b_{ijk} X^i Y^j Z^k,$$

$$M_2(X, Y) = \sum_{i=1}^{q-2} \sum_{j=1}^{q-2} c_{ij} X^i Y^j.$$

In addition,  $T$  is linear if and only if for all  $x, y, z \in \mathbb{F}_q$ ,  $z \neq 0$ , we have

$$xy M_1(x, y, z) = M_2(x, y) M_1(1, M_2(x, y), z). \quad (6)$$

We get an immediate corollary which extends Lemma 12 for linear PTR polynomials.

**Corollary 14.** *For a linear PTR polynomial  $T \in \mathbb{F}_q[X, Y, Z]$  of the form (5), we have*

$$\sum_{i=0}^{q-3} b_{ijk} = \sum_{i=0}^{q-3} b_{jik}$$

for all  $0 \leq j \leq q-3$  and  $1 \leq k \leq q-3$ .

The result follows by substituting  $y = 1$  into (6), whereby one obtains  $xM_1(x, 1, z) = xM_1(1, x, z)$  for all  $x, z \in \mathbb{F}_q$ . This can be viewed as a polynomial equation in  $X, Z$  and the statement of the corollary follows.

## 5 On the Lenz-Barlotti classification and coordinatisation

Let  $\mathcal{P}$  be a projective plane and  $\Gamma$  denote the full collineation group of  $\mathcal{P}$ . If a collineation fixes a line  $\mathcal{L}$  pointwise and a point  $\mathbf{p}$  linewise, then it is called a *central* collineation, and  $\mathcal{L}$  and  $\mathbf{p}$  are called the *axis* and *center* of the collineation, respectively. It is well known that every central collineation in  $\Gamma$  has a unique center  $\mathbf{p}$  and unique axis  $\mathcal{L}$ . Let  $\Gamma(\mathbf{p}, \mathcal{L})$  be the subgroup of  $\Gamma$  consisting of all central collineations of  $\mathcal{P}$  with center  $\mathbf{p}$  and axis  $\mathcal{L}$ . The plane  $\mathcal{P}$  is said to be  $(\mathbf{p}, \mathcal{L})$ -*transitive* if for every two distinct points  $\mathbf{q}, \mathbf{r}$  that are (a) collinear with  $\mathbf{p}$  but not equal to  $\mathbf{p}$ , and (b) not on  $\mathcal{L}$ , there exists a necessarily unique collineation  $\gamma \in \Gamma(\mathbf{p}, \mathcal{L})$  which maps  $\mathbf{q}$  to  $\mathbf{r}$ . Now let  $\mathcal{M}$  be a second line of  $\mathcal{P}$ , not necessarily distinct from  $\mathcal{L}$ . If  $\mathcal{P}$  is  $(\mathbf{p}, \mathcal{L})$ -transitive for all  $\mathbf{p} \in \mathcal{M}$ , then  $\mathcal{P}$  is said to be  $(\mathcal{M}, \mathcal{L})$ -*transitive*; the concept of  $(\mathbf{p}, \mathbf{q})$ -*transitivity* is defined dually. If  $\mathcal{P}$  is  $(\mathcal{L}, \mathcal{L})$ -transitive, then  $\mathcal{L}$  is called a *translation line* and  $\mathcal{P}$  is called a *translation plane* with respect to the line  $\mathcal{L}$ . The definitions of *translation point* and *dual translation plane* are defined dually also.

The Lenz-Barlotti (LB) classification for projective planes is based on the possible sets

$$\mathcal{T} = \{(\mathbf{p}, \mathcal{L}) : \mathcal{P} \text{ is } (\mathbf{p}, \mathcal{L})\text{-transitive}\}$$

of point-line transivities that the full collineation group of a plane can exhibit. Developed by Lenz [10] and refined by Barlotti [1], the classification has a hierarchy of types, starting with little to no point-line transivities in types I and II, through to type VII.2, which represents the Desarguesian plane and where  $\mathcal{T}$  consists of every possible point-line flag. There are no type VI planes at all – the type arises naturally in the study of potential permutation groups, but no plane can exist of this type. For any LB type where a finite example is known, one can also find an infinite example. The converse is not true; infinite examples of types III.1, III.2 and VII.1 are known, while it can be shown that finite examples of each of these types are impossible – in the case of type VII.1,



this is due to the Artin-Zorn Theorem which states any finite alternative division ring is a field, see [8], Theorem 6.20; type III.1 was ultimately resolved by Hering and Kantor [7] and type III.2 was completed by Lüneberg [16] and Yaqub [17]. It should be noted that several finite cases remain open – the question of existence of finite projective planes of LB types I.2, I.3, I.4 and II.2 remains unresolved.

Our motivation for discussing the Lenz-Barlotti types of projective planes is made clear when we return to considering the coordinatisation of planes. In parallel with the Lenz-Barlotti classification, there is a corresponding structural hierarchy for properties of PTRs as one ascends through the Lenz-Barlotti types, though one now assumes that the coordinatisation is done in such a fashion so that the resulting PTR exhibits the most structure. In LB type I.1, the PTR has no additional structure beyond Lemma 1. All other planes can be coordinatised to produce a linear PTR. A LB type II plane can be coordinatised to produce a PTR  $T$  which is linear and where  $\oplus$  is associative (so  $\oplus$  describes a group operation on the coordinatising set  $\mathcal{R}$ ). Any plane which is at least LB type IV is a translation plane. LB type IV planes can be coordinatised to produce quasifields, LB type V planes can produce semifields, and the Desarguesian case, of course, can produce a field. More specifically, we can say the following.

**Lemma 15.** *The following statements hold.*

- (i) *A plane  $\mathcal{P}$  which is only  $((0), [0])$ -transitive is necessarily LB type I.2. The plane  $\mathcal{P}$  is  $((0), [0])$ -transitive if and only if it can be coordinatised by a linear PTR with associative multiplication  $\odot$ . In such cases,  $\Gamma((0), [0])$  is isomorphic to the group described by  $\odot$ . Moreover, during coordinatisation,  $\mathbf{x}$  is chosen to be the point  $(0)$ .*
- (ii) *A plane  $\mathcal{P}$  which is only  $((0), [0])$ -transitive and  $((\infty), [0, 0])$ -transitive is necessarily LB type I.3. The plane  $\mathcal{P}$  is  $((0), [0])$ -transitive and  $((\infty), [0, 0])$ -transitive if and only if it can be coordinatised by a linear PTR with associative multiplication  $\odot$  and displaying a left distributive law.*
- (iii) *A plane  $\mathcal{P}$  which is  $((\infty), [\infty])$ -transitive is necessarily LB type at least II. The plane  $\mathcal{P}$  is  $((\infty), [\infty])$ -transitive if and only if it can be coordinatised by a linear PTR with associative addition  $\oplus$ . In such cases,  $\Gamma((\infty), [\infty])$  is isomorphic to the group described by  $\oplus$ . Moreover, during coordinatisation,  $\mathbf{y}$  is chosen to be the point  $(\infty)$ .*
- (iv) *A plane  $\mathcal{P}$  which is a translation plane or dual translation plane is necessarily Lenz-Barlotti type at least IV. The plane  $\mathcal{P}$  is a translation plane (resp. dual translation plane) if and only if it can be coordinatised by a linear PTR with associative addition  $\oplus$  and a right distributive law  $(x \oplus y) \odot z = x \odot z + y \odot z$  (resp. a left distributive law  $x \odot (y \oplus z) = x \odot y + x \odot z$ ). In such cases, the order of  $\mathcal{P}$  must be a prime power  $q$  and the group described by  $\oplus$  is elementary abelian. Moreover, during coordinatisation,  $\overline{\mathbf{x}\mathbf{y}}$  is the translation line (resp.  $\mathbf{y}$  is the translation point).*

(v) A plane  $\mathcal{P}$  which is both a translation plane and a dual translation plane (so  $[\infty]$  is a translation line and  $(\infty)$  is a translation point) is necessarily Lenz-Barlotti type at least V. The plane  $\mathcal{P}$  is LB type at least V if and only if it can be coordinatised by a linear PTR with associative addition  $\oplus$  and both a left and right distributive law. In such cases, the order of  $\mathcal{P}$  must be a prime power  $q$  and the group described by  $\oplus$  is elementary abelian. Moreover, during coordinatisation, the  $\overline{\mathbf{x}\mathbf{y}}$  is the translation line and  $\mathbf{y}$  is the translation point.

These results come from [3], Chapter 3, and [8], Chapters 5 and 6, and we refer the reader to these references for further information on the Lenz-Barlotti classification and the corresponding properties of PTRs.

This leaves open one obvious question, that of how to coordinatise a plane optimally. Lemma 15 makes clear the following strategy to be used during the coordinatisation process:

- If  $\mathcal{T}$  contains an incident point-line flag, one such flag must be  $((\infty), [\infty])$ .
- If  $\mathcal{T}$  contains a non-incident point-line flag, one such flag must be  $((0), [0])$ .

Unless the plane is LB type I.1, at least one, and possibly both, of these strategems can be met during the initiation phase of the coordinatising process, when one chooses the triangle  $\mathbf{Oxy}$ . In the following, we assume that the planes have been coordinatised optimally with respect to the properties exhibited by the PTR, and in accordance with the above strategy. As part of such an “optimising” strategy, we prioritise associativity of the operations  $\oplus$  and  $\odot$  of the PTR over distributivity whenever there is such a choice available.

This optimal coordinatisation can be exploited even further through the use of Figures 4 or 5. For example, if  $\mathcal{P}$  is  $((\infty), [\infty])$ -transitive and the group  $\Gamma((\infty), [\infty])$  is known, one can use that group as the labelling set and use Figure 4 to ensure that  $\oplus$  is actually the operation of the group. Likewise, if the plane is  $((0), [0])$ -transitive and the group  $\Gamma((0), [0])$  is known, one can use that group, along with an additional element 0, as the labelling set and use Figure 5 to ensure that  $\odot$  is actually the operation of the group. It is for this specific reason that we have taken such care in describing the coordinatisation method and the actions of the two loops on the vertical line in Section 2 – if these actions were not able to be described explicitly, then one could not pursue the optimal coordinatising strategy we’ve outlined.

Linking these optimising strategies to PTR polynomials, the most obvious cases we might be interested in is when either  $\Gamma((\infty), [\infty])$  is elementary abelian, or when  $\Gamma((0), [0])$  is cyclic. In the former case, through optimal coordinatisation, we can assume  $\oplus$  is field addition, while in the latter case, we can force  $\odot$  to be field multiplication through coordinatising optimally. (It should be noted that one cannot simultaneously assume optimal coordinatisation for both  $\oplus$  and  $\odot$  as the labelling of the line  $\overline{\mathbf{Oy}}$  is determined by exactly one of Figures 4 or 5 in these optimising strategies.) In cases where neither of these conditions arise, a representation theory for representing groups by polynomials is needed; such a theory was recently developed by Castillo and the author, see [2].

For the remainder of this article, we consider how knowing either  $\oplus$  or  $\odot$  is a field operation affects the PTR polynomial. We begin first with the case where  $\oplus$  is assumed to be field addition – this situation is actually quite common, especially in the study of semifields, dating back to the first proper examples given by Dickson in [4]. In fact, if the plane is Lenz-Barlotti IV or higher, then you are guaranteed that any optimal coordinatisation will force  $\oplus$  to be field addition.

**Theorem 16.** *Let  $\mathcal{P}$  be a projective plane of order  $q = p^e$  for some prime  $p$  which is  $((\infty), [\infty])$ -transitive and where  $\Gamma((\infty), [\infty])$  is elementary abelian. Suppose  $T \in \mathbb{F}_q[X, Y, Z]$  is a PTR polynomial obtained from coordinatising  $\mathcal{P}$  optimally, so that the resulting additive loop is field addition.*

(i) *If  $\mathcal{P}$  is strictly LB type II.1, then*

$$T(X, Y, Z) = M_2(X, Y) + Z, \quad (7)$$

*where  $M_2(X, Y)$  is as in (5).*

(ii) *If  $\mathcal{P}$  is strictly LB type II.2, then  $T \in \mathbb{F}_q[X, Y, Z]$  is of the shape (7) and where*

$$M_2(x, M_2(y, z)) = M_2(M_2(x, y), z)$$

*for all  $x, y, z \in \mathbb{F}_q$ .*

(iii) *If  $\mathcal{P}$  is a translation plane of LB type at least IV, then  $T \in \mathbb{F}_q[X, Y, Z]$  is of the shape (7) and where*

$$M_2(X, Y) = \sum_{i=0}^{e-1} \sum_{j=1}^{q-1} c_{ij} X^{p^i} Y^j. \quad (8)$$

(iv) *If  $\mathcal{P}$  is a dual translation plane of LB type at least IV, then  $T \in \mathbb{F}_q[X, Y, Z]$  is of the shape (7) and where*

$$M_2(X, Y) = \sum_{i=1}^{q-1} \sum_{j=0}^{e-1} c_{ij} X^i Y^{p^j}. \quad (9)$$

(v) *If  $\mathcal{P}$  is LB type at least V, then  $T \in \mathbb{F}_q[X, Y, Z]$  is of the shape (7) and where*

$$M_2(X, Y) = \sum_{i=0}^{e-1} \sum_{j=0}^{e-1} c_{ij} X^{p^i} Y^{p^j}. \quad (10)$$

*Proof.* By our hypotheses, the plane  $\mathcal{P}$  is necessarily LB type at least II.1, and  $y \oplus z = y + z$ , so that in (4) we see  $M_1 = 0$ . The claim of (i) now follows at once from Theorem 13. Extending to LB type II.2 is immediate from the fact that, in an optimal coordinatisation, the plane will be both  $((\infty), [\infty])$ -transitive and  $((0), [0])$ -transitive, and  $x \odot y = M_2(x, y)$  will act isomorphically to  $\Gamma((0), [0])$ .

Thus the condition given on  $M_2$  is nothing more than the associative property of the operation  $\odot$ .

For (iii), Lemma 15 tells us we must have Equation 7, as well as a right distributive law. Thus  $M_2(X, Y)$  must satisfy  $M_2(a+b, y) = M_2(a, y) + M_2(b, y)$  for all  $a, b, y \in \mathbb{F}_q$ . It follows at once that  $M_2(X, Y)$  is a linearised polynomial in  $X$ . Thus  $M_2$  has the form claimed. A similar argument deals with the case (iv). The claims of (v) now follow at once as a LB type V plane is both a translation plane and a dual translation plane.  $\square$

It is worth noting that whenever we consider a projective plane of LB type at least IV, we are guaranteed that we can obtain a PTR polynomial of one of the shapes (8), (9), or (10), via Lemma 15.

A polynomial  $f \in \mathbb{F}_q[X]$  is called a *complete mapping on  $\mathbb{F}_q$*  if both  $f(X)$  and  $f(X) + X$  are PPs over  $\mathbb{F}_q$ . Complete mappings and their extensions have been studied in several situations. For example, they are connected to the construction of latin squares. Our next result shows how complete mappings arise completely naturally and in numbers when we look at PTR polynomials.

**Lemma 17.** *Let  $\mathcal{P}$  be a projective plane of order  $q = p^e$  for some prime  $p$  which is  $((\infty), [\infty])$ -transitive and where  $\Gamma((\infty), [\infty])$  is elementary abelian. Suppose  $T \in \mathbb{F}_q[X, Y, Z]$  is a PTR polynomial obtained from coordinatising  $\mathcal{P}$  optimally, so that the resulting additive loop is field addition. Then, for any  $a \in \mathbb{F}_q \setminus \{0, 1\}$ , the polynomial  $f_a(X) = M_2(X, a) - X$ , is a complete mapping on  $\mathbb{F}_q$ .*

*Proof.* By Theorem 16, we know  $T(X, Y, Z) = M_2(X, Y) + Z$ . We now appeal to Properties (b) and (c). By Property (c), for  $a, b, c, d \in \mathbb{F}_q$  with  $a \neq c$ , there exists a unique  $x$  satisfying  $M(x, a) + b = M(x, c) + d$ . Setting  $b = 0$ ,  $c = 1$  and appealing to Property (b), we find for all  $a \neq 1$ ,  $M(x, a) - M(x, 1) = M(x, a) - x = d$  has a unique solution in  $x$  for any  $d$ . Thus  $f_a(X) = M(X, a) - X$  is a permutation polynomial over  $\mathbb{F}_q$  for all  $a \neq 1$ . Additionally,  $f_a(X) + X = M(X, a) = T(X, a, 0)$  is a permutation polynomial for all  $a \neq 0$  by Theorem 7 (i).  $\square$

It remains to consider what can be said about PTR polynomials when we know  $\odot$  coincides with field multiplication. Our initial assumption, then, must be that the plane is at least  $((0), [0])$ -transitive. We note that in this case, by starting with a finite projective plane with a non-incident flag transitivity, the only LB types possible are I.2, I.3, I.4, II.2, the planar nearfields of type IV, or VII.2 We may ignore the planar nearfields case, as the multiplicative groups involved in that case are necessarily non-abelian, so can never be cyclic. Since II.2 strictly contains only I.2, in the heirarchy of LB types under consideration, we have two distinct strings:

- I.2  $\subseteq$  I.3  $\subseteq$  I.4  $\subseteq$  VII.2, and
- I.2  $\subseteq$  II.2  $\subseteq$  VII.2.

Furthermore, it was shown by Ghinelli and Jungnickel [5] that I.3 and I.4 planes correspond to the non-abelian and abelian case, respectively, of the same existence problem for neo-difference sets. In particular, by assuming  $x \odot y = xy$ , when we come to consider classes I.3 and I.4, we are enforcing the abelian case; this is why LB type I.3 does not occur in the following statement.

**Theorem 18.** *Let  $\mathcal{P}$  be a projective plane of order  $q = p^e$  for some prime  $p$  which is  $((0), [0])$ -transitive and where  $\Gamma((0), [0])$  is cyclic. Suppose  $T \in \mathbb{F}_q[X, Y, Z]$  is a PTR polynomial obtained from coordinatising  $\mathcal{P}$  optimally, so that the resulting multiplicative loop is field multiplication.*

(i) *If  $\mathcal{P}$  is strictly LB I.2, then*

$$T(X, Y, Z) = Z + XY + XYZ M_1(X, Y, Z), \quad (11)$$

where

$$M_1(X, Y, Z) = \sum_{i,j=0}^{q-3} b_{ij} (XY)^i Z^j.$$

(ii) *If  $\mathcal{P}$  is strictly LB I.4, then  $T$  is of the shape (11) and where*

$$M_1(X, Y, Z) = \sum_{i=0}^{q-3} b_i (XY)^i Z^{q-2-i}.$$

(iii) *If  $\mathcal{P}$  is strictly LB II.2, then  $T$  is of the shape (11) and where*

$$\begin{aligned} & yz + xy M_1(1, x, y) (1 + z M_1(1, x + y + xy M_1(1, x, y), z)) \\ &= xy + yz M_1(1, y, z) (1 + x M_1(1, x, y + z + yz M_1(1, y, z))) \end{aligned}$$

for all  $x, y, z \in \mathbb{F}_q$ .

*Proof.* By hypothesis,  $x \odot y = xy$ , and Lemma 15 tells us the PTR is linear. Thus  $T(x, y, z) = (xy) \oplus z$ , and now an appeal to Theorem 13 produces the first claim, where we define  $b_{ij}$  by  $b_{ij} = b_{iij}$ .

For the second, we use the fact the PTR polynomial  $T$  obtained from optimal coordinatisation must have a left distributive law. Since  $x(y \oplus z) = xy \oplus xz$  for all  $x, y, z \in \mathbb{F}_q$ , we have the identity

$$xyz M_1(1, y, z) = x^2 yz M_1(1, xy, xz)$$

for all  $x, y, z$ . Now this equation has no higher powers of  $y$  or  $z$  beyond the  $(q-2)$ nd, and so we can view this as a polynomial identity in  $Y, Z$ . Equating coefficients, we find for all  $x \in \mathbb{F}_q$  and all  $0 \leq i, j \leq q-3$ ,

$$b_{ij} x = b_{ij} x^{2+i+j}.$$

Thus  $b_{ij} = 0$  unless  $2 + i + j = q$ , which proves we may index the (potentially) non-zero coefficients by a single counter, and this yields the 2nd claim.

For (iii), the proof is essentially the same as for LB type II.2 in Theorem 16, in that we know  $\oplus$  will be associative in an optimal coordinatisation of the plane  $\mathcal{P}$  and the condition on  $M_1$  given above is equivalent.  $\square$

## References

- [1] A. Barlotti, *Le possibili configurazioni del sistema delle coppie punto-retta  $(A, a)$  per cui un piano grafico risulta  $(A, a)$ -transitivo*, Boll. Un. Mat. Ital. **12** (1957), 212–226.
- [2] C. Castillo and R.S. Coulter, *A general representation theory for constructing groups of permutation polynomials*, Finite Fields Appl. **35** (2015), 172–203.
- [3] P. Dembowski, *Finite Geometries*, Springer-Verlag, New York, Heidelberg, Berlin, 1968, reprinted 1997.
- [4] L.E. Dickson, *On commutative linear algebras in which division is always uniquely possible*, Trans. Amer. Math. Soc **7** (1906), 514–522.
- [5] D. Ghinelli and D. Jungnickel, *On finite projective planes in Lenz-Barlotti class at least I.3*, Adv. Geom (2003), suppl., S28–S48.
- [6] M. Hall, *Projective planes*, Trans. Amer. Math. Soc **54** (1943), 229–277.
- [7] C.H. Hering and W.M. Kantor, *On the Lenz-Barlotti classification of projective planes*, Arch. Math. **22** (1971), 221–224.
- [8] D.R. Hughes and F.C. Piper, *Projective Planes*, Graduate Texts in Mathematics, vol. 6, Springer-Verlag, New York, Heidelberg, Berlin, 1973.
- [9] N.L. Johnson, *Fano configurations in translation planes of large dimension*, Note Mat. **27** (2007), 21–38.
- [10] H. Lenz, *Zur Begründung der analytischen Geometrie*, S.-B. Math.-Nat. Kl. Bayer. Akad. Wiss. (1954), 17–72.
- [11] R.W. Matthews, *Permutation polynomials in one and several variables*, Ph.D. thesis, University of Tasmania, Hobart, Tasmania, Australia, 1990.
- [12] G.L. Mullen and D. Panario, *Handbook of Finite Fields*, Discrete Mathematics and Its Applications, vol. 78, Chapman and Hall, CRC Press, 2013.
- [13] H. Neumann, *On some finite non-desarguesian planes*, Arch. Math. **6** (1954), 36–40.
- [14] B. Petrak, *Fano subplanes in finite Figueroa planes*, J. Geom. **99** (2010), 101–106.
- [15] A.J. Rahilly, *The existence of Fano subplanes in generalized Hall planes*, J. Austral. Math. Soc. **16** (1973), 234–238.
- [16] H. Lüneberg, *Zur Frage der Existenz von endlichen projektiven Ebenen vom Lenz-Barlotti-Typ III.2*, J. reine angew. Math. **220** (1965), 63–67.
- [17] J.C.D.S. Yaquib, *The non-existence of finite projective planes of Lenz-Barlotti class III.2*, Arch. Math. **18** (1967), 308–312.